State of Michigan
Business Resumption Plan
Outline

INTRODUCTION

The primary objective of the State of Michigan's Business Resumption Plan is to enable the State to survive a disaster and reestablish normal business operations. In order to survive, State Agencies must ensure critical services can resume normal processing within a reasonable time frame. The goals of Business Resumption Planning are to:

- Identify weaknesses and implement a disaster mitigation program
- Minimize the duration of a serious disruption to business operations
- Facilitate effective coordination of recovery tasks
- Reduce the complexity of the recovery effort
- Document Roles and Responsibilities

Historically, disaster recovery efforts have concentrated on issues that involve technology. Computer applications and the hardware and software required for systems support. Frequently, this has lead to the development of recovery plans that are not fully responsive to the needs of the business supported by those resources. Contingency planning is a business issue. While the Information Technology area addresses the systems side, a second area of great concern needs to have the same attention: Continuation of services provided by the business units. In today's environment the effects of long-term operations outage may have catastrophic impacts. Development of a viable recovery strategy must address the needs of business to continue to provide critical services and maintain systems for resources to enable the continuation of service delivery. When faced with catastrophic events, service delivery must continue, and the business unit must address these needs for inclusion into a comprehensive business resumption plan.

The methodology used to develop business resumption plans emphasize the following:

- Provide management with a comprehensive understanding of the total effort required to develop and maintain an effective Business Resumption, Contingency and Disaster Recovery plan;
- Obtain commitment from appropriate management to support and participate in this;
- Define business resumption, contingency and disaster recovery requirements from the business and service provided perspective;
- Document the impact of an extended loss to operations and key business functions;
- Focus on disaster mitigation, impact minimization and comprehensive recovery;

- Select project teams that ensure the proper balance required for plan development;
- Develop resumption, contingency and recovery plans that are understandable, easy to use and easy to maintain; and
- Define how resumption, contingency and recovery planning are integrated into ongoing business planning and system development processes to ensure the plans remain viable over time.

The aim of the planning process is to:

- Assess existing vulnerabilities;
- Implement disaster avoidance and mitigation procedures; and
- Develop a comprehensive plan that will enable the organization to react appropriately and timely when a disaster strikes.

The methodology for business resumption and contingency planning has several steps designed to facilitate planning, testing and implementation. The steps are described as follows:

STEP 1 – PROJECT INITIATION

Project Initiation is used to obtain an understanding of the existing and projected environment of the agency. This understanding will provide the project team with the opportunity to refine the project scope, develop project schedules; and identify and address any issues that the plan could impact. Two key deliverables of this step are the development of a policy to support the recovery programs, and an awareness program to educate management and staff. Clear communication to all individuals who will be required to participate in the project is important.

STEP 2 - VULNERABILITY ASSESSMENT AND GENERAL DEFINITION OF REQUIREMENTS

From an economic and business strategy perspective, it is preferable to concentrate on activities that have the greatest effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This step addresses measures to reduce the probability of occurrence. This step will include the following key tasks:

- Security Assessment of the business, computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

The Security Assessment will enable the project team to improve any existing emergency plans and disaster mitigation measures and to develop required emergency plans and disaster preventative measures where none exist. Two key deliverables of this step are:

- Presentation of findings and recommendations resulting from the activities of the Security Assessment to agency management for corrective action initiation and timely implementation.

- Formal Scope Definition of the planning effort

    - Analysis and recommendation for the purchase of recovery planning and maintenance software tools required to support development and future maintenance of plans following implementation.

    - Plan Framework Development (State of Michigan, Business Resumption, Contingency and Disaster Recovery Planning guideline).

    - Project Team assembly and commencement of Awareness Program sessions.

STEP 3 - BUSINESS IMPACT ASSESSMENT (BIA)

Business Impact Assessment (BIA) for all business units will enable the project team to identify critical processes, systems, interdependencies, agency priorities, economic impacts resulting from service denial; and determine the threshold for "disaster declaration".

BIA results should be presented to agency management. The results identify critical service functions and time frames for recovery after service interruption. The BIA is then used as bases for identifying systems and resources required for supporting critical services provided by the agency. The key deliverables of this step is the BIA document and recommendations.

STEP 4 - DETAILED DEFINITION OF REQUIREMENTS

Detailed definition requirements leads to the development of recovery profiles. The profiles are used as a basis for analyzing alternative recovery strategies and are developed by identifying resources required to support critical functions identified in Step Three. The profile should include:

- Hardware (mainframe, data and voice communications and personal computers)
- Software (vendor supplied, in-house developed, etc.)
- Data retention requirements and identification of critical records
- Documentation (user, procedures, policies)
- External support (as necessary to continue service provisions)
- Facilities (office space, office equipment, etc.)

- Personnel for each business area

Recovery Strategies should be based on short term, intermediate term and long term outages.

STEP 5 - PLAN DEVELOPMENT

Plan development provides the recovery plans components. The components are defined and plans are created and documented. The plans developed should be presented at a level that allows for execution by those who are assigned responsibility. The agency's organizational structure chart is not an appropriate tool for responsibility assignment in this step. The most qualified person(s) should be identified for the tasks. This step also includes:

- Implementation of changes to user procedures
- Upgrades to existing system processing operational procedures required to support selected recovery strategies and alternatives
- Vendor contract negotiations (with suppliers of recovery services)
- Definition of Recovery Teams, roles and responsibilities
- Development of recovery standards that support Plan Development activities

STEP 6 - VALIDATION

Validation is planning for and testing the business resumption and contingency plans. A comprehensive program is developed during this step. The approach taken to test the plans depends on the strategies selected to meet the recovery requirements of the agency. As the recovery strategies are defined, specific testing plans, exercises and scenarios are developed to ensure written procedures are comprehensive and accurate. The exercise plans and scenarios should:

- Define test purpose and approach
- Identify test teams
- Structure test
- Conduct test
- Analyze results
- Modify plans

Testing cycles are identified based on needs and priorities of the critical services. The testing requirements for the State of Michigan have been identified as semi-annual and interim as needed when new processes are introduced (Business Resumption, Contingency and Disaster Recovery Planning guideline). Rehearsals and full-blown testing should occur where required. Other required activities for this step include:

- Assurance that communication mechanisms are in place and tested (employee notifications)
- Recheck of plans for alignment to objectives and intent

- Establishment of individual and cross-training (external awareness)
- Evaluation of alternative testing strategies
- Budget provisions for plan testing.

Testing strategies tailored to the environment should be selected and an on-going testing program should be established. Validation is a living document. Step must be taken to ensure:

- Plans are truly executable
- Results are evaluated, documented and changes incorporated

STEP 7 - MAINTENANCE

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing Change Management processes are revised to take plan maintenance into account. In areas where change management does not exist, procedures will be recommended and implemented. An ongoing maintenance program should be established that mirrors the validation program. Maintenance is also a living document. Change Management and documentation logs should be utilized for this program.

BEST PRACTICES[1]

For plan development
- Include "return to normalcy" plans
- Use checklists to ensure complete coverage
- Dust off Y2K emergency response plans
- Establish central and distributed storage plans
- Detail procedures for emergency response, recovery, restoration and resumption
- Establish command-and control structure for operations and crisis management
- Complete all detailed documentation

For testing
- Consider level of testing (full, scenarios, role playing)
- Test evacuation plans, calling tree, program units plans and technology plans
- Incorporate full network and data recovery plans
- Retest following an unsuccessful test
- Consider "unscheduled" tests
- Validate off-site data backups semi-annually
- Perform regular testing on critical web servers

For employees
- Training is key for effective employee response
- Educate all employees on the effects of traumatic stress and ways to aid others
- Inventory telecommuters
- Address daily activities (food service, childcare, etc.)

For Business Continuity success
- Ensure everyone knows what is expected of them during a disaster
- Arrange to consult with key employees in their absence
- Maintain current, accurate status information on employees, facilities, and resources
- Identify communications or public relations officer responsible for detailing the "when, where, how and why" and keep records of all information released
- Keep stakeholders informed – be a leader

[1] Best Practices derived from: "How Can I Determine Public-Sector Business Continuity and Disaster Coordination Readiness?" Meta Group Presentation, How-To Teleconference, November 15, 2001.

BUSINESS RECOVERY CHECKLIST[2]

Senior Management	**Financial Management**
❒ Remain visible to employees / stakeholders	❒ Separately track losses / recovery costs
❒ Delegate recovery roles	❒ Formally notify insures of claims
❒ Establish a Recovery Steering Committee	❒ Protect facilities from further damage
❒ Direct manage and monitor the recovery	❒ Seek interim relief from insurers
❒Avoid temptation to participate hands-on	❒ Investigate regulatory relief
❒ Publicly praise successes	❒ Contact analysts / rating agencies
❒ Clearly communicate new roles & responsibilities	❒ Pay current insurance premiums
❒ Rationally amend business plans / projections	Re-establish:
❒ Closely control media / analyst communications	❒ Payroll processes
Human Resources (continuously)	❒ Benefits processes
❒ Re-assess resources versus needs	❒ Accounts payable processes
❒ Monitor productivity of personnel	❒ Billing / accounts receivable processes
❒ Prioritize reallocation of resources	❒ Credit / market risk monitoring
❒ Provide appropriate retraining	❒ External / internal reporting
❒ Monitor employee morale	❒ Key reconciliations
❒ Guard against employee burnout	❒ Other financial controls
❒ Monitor for delayed stress / trauma	❒ Meaningful key performance indicators (KPIs)
❒ Provide counseling and support	❒ Transaction controls / limits
❒ Pay employees / beneficiaries timely	❒ Authorities / approvals limits
Technology / Management	Re-assess:
❒ Identify / prioritize mission critical applications	❒ Cash flow projections
❒ Prepare business impact analysis by unit	❒ Budget / budgeting process
❒ Re-assess original recovery plans	❒ Closing process / timing
❒ Continuously assess recovery site stability	**Business Operations**
❒ Recover / reconstruct all critical data	❒ Assess ability to deliver customer orders
Within the recovery environment:	❒ Identify outsourcing opportunities
❒ Assess adequacy of information security	❒ Refresh supply chain management
❒ Assess the adequacy of system security	❒ Analyze lease requirements / options
❒ Re-assess recovery tolerance / timeframes	❒ Establish new risk-mitigating controls
❒ Evaluate recovery contingencies	❒ Amend policies and procedures
❒ Develop and test recovery plans	❒ Develop meaningful KPIs
❒ Develop emergency plans for recovery staff	Continuously re-assess the adequacy of:
Customers, Clients and Suppliers	❒ Recovery site
❒ Re-establish customer / vendor contacts	❒ Existing plant and equipment
❒ Reconsider revenue / profit projections	❒ Production capacity
❒ Recover / reconstruct contracts / customer data	❒ Communications / sales capacity
In the post-disaster environment, assess:	❒ Transaction settlement processes
❒ Changed customer requirements	
❒ Ability to respond to customer requests / inquires	
❒ Changed customer / supplier market behavior	
❒ Appropriate products / product mix	
❒ Customer / counterparty stability	
❒ Supplier / vendor reliability	
❒ Status of existing orders / contracts	

[2] Ms. Michael C. Redmond and James Hammill, "The Challenge of Getting Back To Business," Disaster Recovery Journal, Winter 2002, Volume 15, Number 1, p. 92.